UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/518,639	12/20/2004	Nathalie Feyt	1032326-000288	4953

21839 7590 12/24/2008
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
SU, SARAH	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
12/24/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPFDD@bipc.com

Office Action Summary	Application No.	Applicant(s)	
	10/518,639	FEYT ET AL.	
	Examiner	Art Unit	
	Sarah Su	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 September 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 September 2008* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *9/15/08*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

FINAL ACTION

1. Amendment A, received on 15 September 2008, has been entered into record. In this amendment, claims 1-18 have been amended.

2. Claims 1-18 are presented for examination.

Response to Arguments

3. The application has complied with the examiner's request to submit a new oath or declaration and it is now in compliance.

4. Regarding the objections to the specification, the applicant has amended the specification, and the examiner hereby withdraws the objections.

5. Regarding the objections to the claims, the applicant has amended the claims, and the examiner hereby withdraws the objections.

6. Regarding the objections to the drawings, the applicant has submitted a replacement sheet filed 15 September 2008, and the examiner hereby withdraws the objections.

7. Applicant's arguments with respect to the rejection under 35 USC 101 and 112 1st paragraph of claims 13 and 14 have been fully considered and are persuasive. The rejection of claims 13 and 14 has been withdrawn.

8. Applicant's arguments with respect to the rejections under 35 USC 103 filed 15 September 2008 have been fully considered but they are not persuasive.

As to claim 1, it is argued by the applicant that Futa does not disclose where pairs of prime numbers (p, q) are calculated and stored independent of knowledge of

the pair of values (e, l). The examiner respectfully disagrees. Futa discloses the prime numbers are generated using a random number (col. 9, lines 3-4) and that the bit size of prime p is to be twice the size of prime q (col. 9, lines 41-43). Futa also discloses that the public key is calculated from the prime numbers (col. 11, lines 6-10, 13-14). Therefore, since the public key is calculated after the prime numbers have been calculated, the generation of the prime numbers is not made with knowledge of the public key (i.e. e, l).

As to claim 12, it is argued by the applicant that Hopkins does not disclose means for receiving at least one pair of values (e, l). The examiner respectfully disagrees. Hopkins discloses that a public key is publicly known (0006, lines 12-13) and that a recipient publishes the key, making it known at least to the sender (0006, lines 17-19). Also, Hopkins discloses that a set of cryptographic parameters includes a length of a modulus (i.e. l) and an associated public exponent value (i.e. e) (0083, lines 5-10) and that these cryptographic parameters may be accessed from memory for use in an application where the application may be running on a different system that is communicatively coupled via a modem (0085, lines 5-11).

Information Disclosure Statement

9. The information disclosure statement (IDS) submitted on 15 September 2008 is being considered by the examiner.

Drawings

10. The drawings were received on 15 September 2008. These drawings are acceptable.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 1-6, 8-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Futa et al. (US Patent 7,130,422 B2 and Futa hereinafter) in view of Hopkins et al. (US 2005/0190912 A1 and Hopkins hereinafter).

As to claims 1 and 12, Futa discloses a system and method for prime number generation for information security, the system and method having:

a memory for storing the results of: calculating pairs of prime numbers (p,q) or values representative of pairs of prime numbers, this calculation being independent of knowledge of the pair of values (e,l) in which e is a public exponent and l is the length of the key of the cryptography method (col. 8, lines 56-57, 62-64; col. 9, lines 44, 54-56; col. 10, lines 8, 10, 41-43);

a program for calculating a key d from the stored results and knowledge of a received pair of values (e,l) (col. 1, lines 65-67).

Futa does not disclose:

communication means for receiving at least one pair of values (e,l).

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Futa, as evidenced by Hopkins.

Hopkins discloses a system and method for pre-computing and storing multiple cryptographic keys, the system and method having:

communication means for receiving at least one pair of values (e, l) (0006, lines 9-10, 17-20; 0085, lines 5-11).

Given the teaching of Hopkins, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Futa with the teachings of Hopkins by providing for a way to receive a public key. Hopkins provides motivation by disclosing that a typical cryptographic scheme is a public key system such as RSA, where a public key that is publicly known is needed to encrypt a message and a private key is needed to decrypt a message (0006, lines 5-8). Therefore, in order to implement an RSA-type scheme as claimed, a public key would need to be provided. It is obvious that the teachings of Futa would have benefited from the teachings of Hopkins by providing for a way to receive public key parameters in order to encrypt a message so that a public key cryptographic system can be implemented.

As to claim 2, Futa does not disclose:

> **wherein step A-1) comprises calculating pairs of prime numbers (p, q) without knowledge of the public exponent e or of the length l of the key, using a parameter Π which is the product of small prime numbers, so that each pair (p, q) has a maximum probability of being able to correspond to a future pair (e,l) and can make it possible to calculate the key d.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Futa, as evidenced by Hopkins.

Hopkins discloses:

> **wherein step A-1) comprises calculating pairs of prime numbers (p, q) without knowledge of the public exponent e or of the length l of the key, using a parameter Π** (i.e. n) **which is the product of small prime numbers** (i.e. p_1, p_2, ...) (0057, line 16)**, so that each pair (p, q) has a maximum probability of being able to correspond to a future pair (e,l) and can make it possible to calculate the key d** (0068, lines 1-4)**.**

Given the teaching of Hopkins, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Futa with the teachings of Hopkins by creating a pair of prime numbers based on other prime numbers that can be used to create a key. Hopkins recites motivation by disclosing that latency time can be reduced while maintaining security by pre-computing cryptographic parameters (0033, lines 1-5; 0035, lines 5-6) and that these parameters can be used to calculate a key It is obvious that the teachings of

Hopkins would have improved the teachings of Futa by calculating prime numbers that are used to calculate a key are based on other pre-computed parameters in order to reduce latency time in comparison with conventional cryptographic key generation.

As to claim 3, Futa does not disclose:

> **wherein the calculation of step A-1) also takes account of the fact that e has a high probability of forming part of the set {3, 17, . . . , 2^{16}+1}, and using a seed σ in the calculation which makes it possible to calculate a representative value constituting an image of the pairs (p, q).**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Futa, as evidenced by Hopkins.

Hopkins discloses:

> **wherein the calculation of step A-1) also takes account of the fact that e has a high probability of forming part of the set {3, 17, . . . , 2^{16}+1}** (0127, lines 3-5)**, and using a seed σ in the calculation which makes it possible to calculate a representative value constituting an image** (i.e. prime number value) **of the pairs (p, q)** (0041, lines 1-4).

Given the teaching of Hopkins, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Futa with the teachings of Hopkins by using a seed to calculate cryptographic parameters that represent the prime numbers. Hopkins recites motivation by disclosing that using a random seed ensures that there is no correlation between

prime numbers that are pre-computed, thus maintaining security while providing minimal latency (0041, lines 6-8) and fast encryption. It is obvious that the teachings of Futa would have benefited from the teachings of Hopkins by using a seed to calculate a value representative of prime numbers in order to ensure that the prime numbers are not correlated while providing for fast encryption and minimal latency time.

As to claim 4, Futa does not disclose:

wherein the storage step A-2) comprises storing the image of the pairs.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Futa, as evidenced by Hopkins.

Hopkins discloses:

wherein the storage step A-2) comprises storing the image (i.e. cryptographic parameters) **of the pairs** (0035, lines 23-24)**.**

Given the teaching of Hopkins, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Futa with the teachings of Hopkins by providing for storing cryptographic parameters that are to be used to generate keys. Hopkins recites motivation by disclosing that the cryptographic parameters are stored so that they can be later accessed and provided with minimal latency (0037, lines 1-7). It is obvious that the teachings of Hopkins would have improved the teachings of Futa by storing parameters that are used in the cryptographic process so that they can be later

accessed for usage in order to decrease the latency time by eliminating the need to calculate the parameters when requested.

As to claims 5 and 16, Futa does not disclose:

wherein step A-1) comprises calculating pairs of prime numbers (p, q) for different probable pairs of values (e,l).

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Futa, as evidenced by Hopkins.

Hopkins discloses:

wherein step A-1) comprises calculating pairs of prime numbers (p, q) for different probable pairs of values (e,l) (0035, lines 5-8).

Given the teaching of Hopkins, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Futa with the teachings of Hopkins by using different prime numbers for different public key values. Hopkins recites motivation by disclosing that in a typical cryptographic public key system, it is computationally difficult to determine the private key from the public key (0006, lines 26-27). According to the invention of Hopkins, this is done by ensuring that the prime numbers are relatively prime to e (0057, lines 10-11). Therefore, these prime numbers correspond to different values of e. It is obvious that the teachings of Futa would have benefited from the teachings of Hopkins by providing a pair of prime numbers for different values of (e, l) in order to increase security by ensuring that the numbers are relatively prime.

As to claim 6, Futa discloses:

wherein the parameter Π (i.e. R) **contains the values 3, 17** (i.e. small primes, L_1, L_2,...) (col. 9, line 43; col. 10, line 8). The examiner asserts that because Futa discloses that the parameter Π consists of small prime numbers, then the numbers 3 and 17 may be included because they can be considered small prime numbers.

As to claim 13, Futa discloses:

a calculation means configured to calculate said results stored in memory, the calculation of said results being separate in time from the calculation of the key d (col. 8, lines 56-57, 62-64; col. 9, lines 44, 54-56; col. 10, lines 8, 10, 41-43).

As to claims 8, 14 and 17, Futa discloses:

2) selecting a number j within the range of integers {v, ... , w-1} and calculating l=jΠ (i.e. l=R, j=R', Π =L1×L2×...) (col. 9, lines 54-56; col. 10, line 8);

4) calculating q (i.e. P_a/P_b) **=k+l** (col. 8, lines 56-57, 62-64; col. 10, lines 10, 41-43);

5) verifying that q is a prime number, if q is not a prime number then: a) taking a new value for k using the following relation: k=a k (mod Π); a

belonging to the multiplicative group Z^*_{Π} of integers modulo Π;

b) repeating the method from step 4) (col. 10, lines 25-28).

Futa does not disclose:

1) calculating parameters v and w from the following relations and storing them:

$v=\sqrt{2^{2lo-1}}/\Pi$

$w=2^{2lo}/\Pi$

in which Π is stored and corresponds to the product of the f smallest prime numbers, f being selected such that $\Pi \leq 2^{Bo}$;

3) selecting and storing a prime number k of short length compared to the length of an RSA key within the range of integers {0, . . ., Π-1}, (k, Π) being co-prime.

Nonetheless, these features are well known in the art and would have been an obvious modification of the teachings disclosed by Futa, as evidenced by Hopkins.

Hopkins discloses:

1) calculating parameters v and w from the following relations and storing them:

$v=\sqrt{2^{2lo-1}}/\Pi$

$w=2^{2lo}/\Pi$

in which Π (i.e. n) **is stored and corresponds to the product of the f smallest prime numbers, f** (i.e. k) **being selected such that $\Pi \leq 2^{Bo}$** (i.e. 2^L) (0057, line 16; 0062, line 4)**;**

3) selecting and storing a prime number k of short length compared to the length of an RSA key within the range of integers {0, . . ., Π-1}, (k, Π) being co-prime (0057, lines 10-12).

Given the teaching of Hopkins, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Futa with the teachings of Hopkins by calculating parameters that are used to determine prime numbers for an RSA-type cryptographic system. Hopkins recites motivation by disclosing that the prime numbers must be distinct and suitable for use in the multi-prime cryptographic system (0058, lines 6-9). It is disclosed that the composite number n provides a modulus for encoding and decoding operations (0058, lines 1-2) and that the prime numbers must fall in a certain range, which, alternatively, ensures that the prime numbers and exponent are relatively prime (0063, lines 1-4). It is obvious that the teachings of Futa would have been improved by the teachings for Hopkins by calculating and using parameters for determining prime numbers in such a way that would ensure distinctness and suitability in the system.

As to claim 9, Futa does not disclose:

wherein the numbers j and k can be generated from the seed σ stored in memory.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Futa, as evidenced by Hopkins.

Hopkins discloses:

wherein the numbers j and k can be generated from the seed σ stored in memory (0041, lines 1-6).

Given the teaching of Hopkins, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Futa with the teachings of Hopkins by using a seed to calculate cryptographic parameters that represent the prime numbers. Hopkins recites motivation by disclosing that using a random seed ensures that there is no correlation between prime numbers that are pre-computed, thus maintaining security while providing minimal latency (0041, lines 6-8) and fast encryption. It is obvious that the teachings of Futa would have benefited from the teachings of Hopkins by using a seed to calculate a value representative of prime numbers in order to ensure that the prime numbers are not correlated while providing for fast encryption and minimal latency time.

As to claims 10 and 18, Futa discloses:

where the prime number p is generated by repeating all the above sub-steps while replacing q with p and replacing l_o (i.e. L_{enq}) **with l-l_o** (i.e. L_{enq}') (col. 8, lines 55-57, 61-64; col. 9, lines 19-25). The examiner asserts that because Futa discloses that the prime numbers p_a and p_b are generated using the same unit, then they can be said to be generated using the same steps.

As to claims 11, Futa discloses:

calculating the key d from the pair (p,q) obtained (col. 1, lines 65-67).

Futa does not disclose:

step B comprises, for a pair (p,q) obtained in step A:

verifying the following conditions:

(i) p-1 and q-1 are prime numbers with a given e;

(ii) N=p*q is an integer of given length l;

if the pair (p,q) does not satisfy these conditions: selecting another pair and repeating the verification until a pair is suitable.

Nonetheless, these features are well known in the art and would have been an obvious modification of the teachings disclosed by Futa, as evidenced by Hopkins.

Hopkins discloses:

step B comprises, for a pair (p,q) obtained in step A:

verifying the following conditions:

(i) p-1 and q-1 are prime numbers with a given e (0063, lines 3-4);

(ii) N=p*q is an integer of given length l (0057, lines 11-12);

if the pair (p,q) does not satisfy these conditions: selecting another pair and repeating the verification until a pair is suitable (0058, lines 6-9).

Given the teaching of Hopkins, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Futa with the teachings of Hopkins by choosing different pairs of numbers until certain conditions are met. Hopkins provides motivation by disclosing that high security may be maintained by determining minimal correlation (i.e. relatively prime) (0046, lines 4-6) and that searching may be done faster and more efficiently

when specifying more numbers of smaller length in comparison with the classic two-prime system which uses two numbers of larger length (0079, lines 9-14, 16-20). If the numbers do not follow the specifications, then they must be rejected as suitable (0063, lines 5-6). It is obvious that the teachings of Hopkins would have improved the teachings of Futa by specifying requirements for the numbers that must be met in order to ensure security in the system that can be accomplished quickly and efficiently.

As to claim 15, Futa discloses:

where said object is a chip card (10, Figure 1).

13. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Futa in view of Hopkins as applied to claim 1 above, and further in view of Matyas (US Patent 4,736,423).

As to claim 7, Futa in view of Hopkins does not disclose:

wherein step A-1) comprises an operation of compressing the calculated pairs (p,q) and step A-2) comprises storing the compressed values thus obtained.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Futa in view of Hopkins, as evidenced by Matyas.

Matyas discloses a system and method for reducing RSA crypto variable storage, the method having:

wherein step A-1) comprises an operation of compressing the calculated pairs (p,q) and step A-2) comprises storing the compressed values thus obtained (col. 8, lines 65-68; col. 9, lines 1-2).

Given the teaching of Matyas, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Futa in view of Hopkins with the teachings of Matyas by providing for compression of the numbers and storing the result. Matyas recites motivation by disclosing that efficiently storing parameters required for public key algorithms (through a method such as compression) would allow the system to be implemented where storage is limited (such as a magnetic strip card) (col. 3 lines 55-58). It is obvious that the teachings of Matyas would have improved the teachings of Futa in view of Hopkins by compressing parameters used in public key algorithms in order to save space so that the algorithm may be used in conditions where the storage is limited.

Prior Art Made of Record

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Walker et al. (US Patent 5,884,270) discloses a system and method for facilitating searches using anonymous communications that require key pairs such as with RSA.

Conclusion

15. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sarah Su whose telephone number is (571) 270-3835. The examiner can normally be reached on Monday through Friday 7:30AM-5:00PM EST..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Sarah Su/
Examiner, Art Unit 2431

/Christopher A. Revak/
Primary Examiner, Art Unit 2431